Cybersicurezza : al centro dell'industria del ransomware

WHITE PAPER



STORMSHIELD

Gli attacchi ransomware sono in aumento e minacciano l'equilibrio economico e la longevità di numerose aziende e organizzazioni. Non passa settimana senza che un'impresa o amministrazione venga attaccata e riceva una richiesta di riscatto.

In 30 anni siamo passati da un programma malevolo su floppy disk che esigeva un centinaio di dollari a un'industria criminale strutturata che estorce milioni ogni anno. Ma quali sono le attuali modalità operative dei gruppi di ransomware? In che modo i criminali informatici li impiegano nelle organizzazioni? Dall'interruzione o addirittura cessazione dell'attività alla divulgazione di dati: quali tattiche di pressione utilizzano? E soprattutto, come proteggersi?

In questo white paper analizziamo l'evoluzione del ransomware e gli attori che lo rendono una minaccia da non sottovalutare. Scopriremo il funzionamento di tali malware e forniremo una serie di buone pratiche per evitarne le conseguenze. Tutto ciò senza tralasciare la questione centrale che accomuna diverse strutture che si trovano ad affrontare il problema: pagare o non pagare? Bisogna arrendersi?

01. Dal ricatto al singolo al Big Game Hunting: il ransomware di ieri e di oggi

08 — Le origini “pre-Internet” (1989 - 2006)
10 — Una diffusione che viaggia “nella rete” (2007-2013)
12 — Le prime rivoluzioni tecnologiche (2013 - 2016)
14 — I primi attacchi governativi su scala globale (2017-2018)
16 — L’era del Big Game Hunting (2019-2021)
18 — Verso la strutturazione di una rete cybercriminale (2021-2022)

02. Prezzi e danni: quali sono le conseguenze di un attacco ransomware?

22 — Chi trae vantaggio dagli attacchi ransomware?
26 — Chi sono le vittime?
28 — Quali sono gli effetti sulle strutture coinvolte?
30 — Pagare o non pagare? Bisogna cedere?

03. Come funziona un ransomware: la meccanica dei fluidi

36 — Itinerario del ransomware
38 — Focus sull’accesso iniziale

04. Quali sono le strategie da mettere in atto per smantellare questo meccanismo fraudolento?

44 — Proteggersi prima di un attacco ransomware
44 — Limitare i danni durante un attacco ransomware
44 — Riprendersi da un attacco ransomware

05. Che futuro si prospetta per il ransomware?

48 — Quali caratteristiche avrà il ransomware di domani?
50 — Quali soluzioni attendersi?



Dal ricatto al singolo al *Big Game Hunting*: il ransomware di ieri e di oggi

Essendo lo strumento più diffuso tra i criminali informatici, il ransomware può mettere in crisi qualsiasi azienda o comunità, indipendentemente dalle sue dimensioni e dal suo livello di sicurezza. Come si è evoluta questa minaccia negli ultimi 30 anni? Uno sguardo su un fenomeno in continua evoluzione.

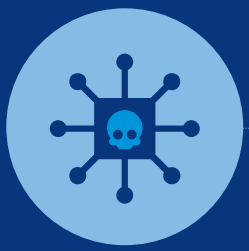
L'evoluzione del ransomware nel corso del tempo



1989-2006

LE ORIGINI "PRE-INTERNET"

AIDS TROJAN, PGPCODER



2007-2013

UNA DIFFUSIONE CHE VIAGGIA "NELLA RETE"

WINLOCK



2013-2016

LE PRIMERIVOLUZIONI TECNOLOGICHE

CRYPTOLOCKER, SYPENG



2019-2021

L'ERA DEL BIG GAME HUNTING

MAZE



2017-2018

I PRIMI ATTACCHI GOVERNATIVI SU SCALA GLOBALE

WANNACRY, NOTPETYA.



2021-2022

VERSO LA STRUTTURAZIONE DI UNA RETE CYBERCRIMINALE

RANSOMWARE-AS-A-SERVICE.

1.1
Le origini « pre-Internet » (1989 - 2006)



1989

I primi ransomware hanno fatto il loro ingresso alla fine degli anni ‘80. Questi programmi malevoli avevano un’unica missione: bloccare il funzionamento della postazione di lavoro nelle aziende e dei (rari) utenti privati dotati di microcomputer.

Ma i ransomware all’epoca erano facilmente rintracciabili grazie alle informazioni sui pagamenti. Solo quindici anni dopo, con l’emergere delle valute digitali, si è assistito a una vera e propria proliferazione di tali minacce.
Tra i primi ransomware distribuiti via Internet, PGPCoder, o “il ransomware da 20 dollari”, mirava a infettare i sistemi Windows già nel 2005 prendendo di mira file con estensioni comuni come .rar, .zip, .jpg, .doc o .xls. —

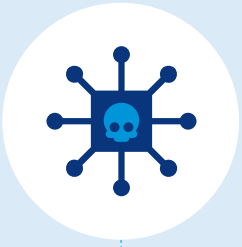
DATA CHIAVE

Il primo ransomware, “AIDS Trojan”, è stato introdotto nel 1989 tramite floppy disk. Il suo compito era quello di criptare i file delle macchine infettate dopo un certo numero di riavvii e richiedere alle vittime il pagamento di un riscatto di 189 dollari per recuperare i dati.

2007-2013

Una diffusioneche viaggia “nella rete”

1.2 Una diffusione che viaggia “nella rete” (2007-2013)



Scareware

Con l'adozione di messaggistica istantanea, social network, forum e reti *peer-to-peer*,il ransomware sta beneficiando di nuovi canali di distribuzione. WinLock, ad esempio, aveva la particolarità di non criptare i dati sul computer infetto. Bloccava l'accesso alla macchina visualizzando una finestra contenente un'immagine pornografica e una richiesta di denaro tramite un servizio SMS a pagamento.

Questa prima evoluzione nel funzionamento del ransomware è chiamata "locker" in riferimento al suo obiettivo: bloccare l'avvio del sistema operativo.

Nello stesso periodo sono emerse varianti che si spacciavano per forze dell'ordine, come il ransomware Reveton nel 2012. Distribuito su piattaforme *peer-to-peer* si spacciava per l'FBI bloccando i computer delle vittime e chiedendo il pagamento di una "multa" di 200 dollari.

Successivamente, le richieste di riscatto sono diventate sempre più creative per aumentare le possibilità di successo. —



PAROLA CHIAVE

Scareware: sistema di ricatto di tipo falso antivirus, molto popolare negli anni 2010.

2013-2016

Le prime rivoluzioni tecnologiche

1.3 Le prime rivoluzioni tecnologiche (2013-2016)



Il ransomware CryptoLocker, con il suo server di command & control che consente di dialogare con la vittima, ha rappresentato una svolta tecnologica nel 2013, esercitando una pressione ancora maggiore. È stato anche uno dei primi ransomware a richiedere un riscatto in bitcoin.

Le criptovalute, infatti, completano un'altra tappa fondamentale nell'evoluzione del ransomware. Con esse - e soprattutto con l'avvento del Bitcoin - l'anonimizzazione dei destinatari dei fondi rende irrintracciabile la richiesta di riscatto. Allo stesso tempo, ransomware come Sypeng hanno sferrato i primi attacchi a tablet e smartphone Android nel 2014 attraverso falsi messaggi di aggiornamento del software Adobe Flash. Nel 2016 è iniziata l'era degli attacchi di phishing con Petya, il cui obiettivo sono gli indirizzi e-mail aziendali celandosi all'interno di un documento Word o PDF. —



27 m$

CIFRE SALIENTI

Questo è l'importo generato da CryptoLocker nei primi due mesi di attività.

2017-2018

I primi attacchi governativi su scala globale

1.4
I primi attacchi governativi su scala globale (2017-2018)



In seguito alla pubblicazione delle vulnerabilità Zero-day sottratte a un'agenzia governativa statunitense, gli attacchi ransomware stanno migliorando la propria capacità tecnica di propagazione: in presenza di reti coesistenti, si diffondono massicciamente da un'azienda all'altra.

WannaCry è stato lanciato nel 2017 e ha riscosso un'ampia copertura mediatica. In poche settimane ha colpito 300.000 computer in 150 Paesi, diffondendosi nei sistemi operativi Microsoft Windows attraverso la vulnerabilità EternalBlue.

A distanza di pochi mesi, alcuni degli elementi fondanti di WannaCry (exploit EternalBlue, spostamento laterale) sono stati reimpiegati dal ransomware NotPetya nel contesto del conflitto di stato tra Russia e Ucraina. Vera e propria arma di distruzione digitale, questo ransomware ha anche camuffato tentativi di sabotaggio della metropolitana ucraina[1], dell'aeroporto di Kiev, della centrale nucleare di Chernobyl[2], della banca centrale e dell'operatore energetico nazionale. Ancora oggi, soggetti come il gruppo cinese Bronze Starlight continuano a servirsi di campagne ransomware per nascondere operazioni di spionaggio.

Nel 2018, il mondo della cybersicurezza è venuto a conoscenza del ransomware Ryuk, che prende di mira soprattutto le grandi aziende. Tutto ciò non lascia presagire nulla di buono per il futuro...

"Il ransomware era solo uno strumento di facciata. Il vero scopo di NotPetya non era l'estorsione, ma la distruzione dei dati, e questo su scala molto ampia, prendendo di mira un intero Paese. "

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

1.5 L'era del Big Game Hunting (2019-2021)



Leakware

Entro la fine del 2019, il numero di attacchi ransomware aumenterà del 365%. Per evitare il rischio di essere intercettati dagli strumenti di sicurezza, i criminali informatici stanno abbandonando le campagne su larga scala (come WannaCry) **per concentrarsi sulle grandi aziende**.

Questo modus operandi, basato sul riconoscimento dell'ambiente e sullo sviluppo di scenari di attacco avanzati, è chiamato big game hunting (caccia grossa). Una strategia che ha dato i suoi frutti, poiché l'importo medio delle richieste di riscatto è quasi triplicato durante il periodo, passando da 13.000 a 36.000 dollari[3].

In questo frangente compare anche il meccanismo della doppia estorsione. L'azienda vittima non solo riceve una richiesta di riscatto, ma viene anche minacciata di rivendere i suoi dati nel dark web. Se questo ricatto non è sufficiente a convincere i più restii a pagare , i cybercriminali rivelano parte dei dati critici rubati (codice sorgente, dati dei clienti). Alcuni si spingono fino a minacciare i clienti finali o i pazienti di queste organizzazioni di divulgare i loro dati personali: si tratta di una triplice estorsione.

Tra questi, troviamo i presunti autori del ransomware Maze. La sua particolarità? Una comunicazione continua con le vittime al fine di esercitare una pressione costante.

Nel 2020, l'attacco di Darkside al gigante statunitense del trasporto e della distribuzione del petrolio Colonial Pipeline arricchisce ulteriormente lo scenario del *big game hunting*. Il ransomware, che tecnicamente è simile a REvil, richiede un riscatto di 5 milioni di dollari. —

"Quando la pressione indotta dalla crittografia non è sufficiente, i gruppi di ransomware passano all'estorsione minacciando di diffondere i dati esfiltrati. E come se non bastasse, utilizzano anche attacchi DDoS per costringere le vittime a pagare. "

ÉDOUARD SIMPÈRE — RESPONSABILE CYBER THREAT INTELLIGENCE, STORMSHIELD

PAROLA CHIAVE

Modulo presente nei ransomware più recenti per il furto dei dati.

DA NOTARE

Una pressione sempre maggiore. Il gruppo ALPHV/ BlackCat pubblica i dati trafugati sul proprio sito .onion, ma anche su un sito web standard il cui nome di dominio contiene quello dell'azienda bersaglio. È facilmente consultabile e include anche una funzione di ricerca per consentire ai clienti di verificare autonomamente il furto dei propri dati.

2012-2022

Verso la strutturazione di una rete cybercriminale

1.6 Verso la strutturazione di una rete cybercriminale (2021-2022)



L'emergere di piattaforme Ransomware-as-a-Service (RaaS) costituisce l'ultima rivoluzionaria novità nel modus operandi di questi cybercriminali. I gruppi di aggressori meno esperti reperiscono ransomware white-label per campagne "chiavi in mano". A fronte di una percentuale del riscatto, ottengono l'infrastruttura completa di una soluzione malevola sviluppata da altri gruppi di criminali informatici. Un settore strutturato, quindi, in cui ognuno ha un ruolo ben definito.

Nel 2021 fanno la loro comparsa gli Initial Access Broker (IAB). In qualità di specialisti delle intrusioni, vendono l'accesso alle reti aziendali ad altri gruppi criminali, che poi lo utilizzano per portare a termine i propri attacchi.

Questa crescente sofisticazione della catena di attacco si spiega con il miglioramento del livello di protezione delle aziende. Purtroppo, l'industrializzazione del ransomware sta comportando anche una riduzione dei tempi di implementazione[5]. Al punto che alcuni non si preoccupano più di seguire tutti i passaggi:Nel marzo 2022, un gruppo di cybercriminali iraniani[6] ha inviato la propria richiesta di riscatto alla stampante locale di un governo statunitense senza prima criptare i terminali. —

DATA CHIAVE

La Casa Bianca ha riunito decine di Paesi, tra cui Francia e Germania, in un vertice di due giorni volto a individuare soluzioni al problema globale del ransomware. Ma è sufficiente per affrontare finalmente il problema in modo diretto?

CIFRE SALIENTI

X2

Nel 2021 gli attacchi ransomware sono raddoppiati a livello globale[4].

PER APPROFONDIRE

BREVE STORIA DEL RANSOMWARE

Per saperne di più sulla "breve" storia del ransomware, consultate il nostro articolo dedicato[7].

Ottobre 2022


[error] malicious code logged (trigger.warning)
m#4:80a?:/q.s status.command if ("true") add string
ocal.config = (245,23,068,789,a48) [lock.command]
{logged: # input.new (c
= address [statu
denial // scri
]e] {?unkno
n logged: #
n logged: #
m#4:80a?:
cal.config
mn4:h61l0
s?] code<
src=[error]
m#4:80a?:/
cal.confi
false fun
{logged:
address
denial //
?] {?unk
logged: #
logged: #
logged: # inp
m#4:80a?:/q.s statu
al.config = (245,23,
mn4:h61l04y} name<i
?] code< [true] # status (m#4:80a?:/q.s) {logged
rc=[error] malicious code logged (trigger.warning)
status.command if ("true") add string
(245,23,068,789,
name<img>=spa
put.new(create)}
atus?] code< [tr
t src=[erro
statu
onfig sc
onfig sc
onf sc
ue") add st
k.command]
ress logged <[#]
ent.name[get]
tus (m#4:80a?
de logged {t

Prezzi e danni: quali sono le conseguenze di un attacco ransomware?

Un attacco ransomware raramente è privo di conseguenze per le vittime. Oltre alle perdite finanziarie, si destabilizza l'intera catena del valore delle organizzazioni. Analizziamo in dettaglio i meccanismi di un attacco, i relativi prezzi e i danni.

2.1 Chi trae vantaggio dagli attacchi ransomware?

Negli ultimi tre decenni, il mondo del ransomware è diventato sempre più strutturato. Le bande di criminali informatici vanno e vengono, ma la loro crescente competenza non è più in discussione.



I gruppi di ransomware sono suddivisi in diverse "famiglie", diffuse in tutto il mondo. Delle 100 famiglie o varianti identificate dall'FBI[8], molte provengono da gruppi con sede in Asia e in Europa orientale. In Europa sono attivi oltre una trentina di gruppi di ransomware, sotto i tristemente noti nomi LockBit, Conti, ALPHV/BlackCat o anche Hive.

Spesso legati agli eventi geopolitici attuali, i gruppi di cybercriminali compaiono e scompaiono ad un ritmo incalzante. Dopo aver dichiarato il proprio sostegno alla Russia, il gruppo Conti ha subito una serie di fughe di dati: sono stati divulgati i registri delle discussioni interne, il codice sorgente e altri file utilizzati dal gruppo. Ha chiuso il suo sito vetrina nel 2022[9] ; Ma potrebbe riapparire in altre forme, come lasciano presagire i segnali lanciati dalla sua filiale Karakurt nel mese di giugno[10]. Tutto ciò richiama alla mente il caso del gruppo REvil, smantellato nel gennaio 2022 e tornato alla ribalta pochi mesi dopo[11].

In breve, l'industria del malware si sta strutturando e con essa emerge una vera e propria economia parallela delle minacce informatiche, con diverse figure professionali. Lo sviluppo del mercato degli attacchi informatici è tale che *"possiamo ormai parlare di un'economia parallela"* spiega Sébastien Viou, Direttore della sicurezza informatica dei prodotti e cyber-evangelista presso Stormshield. —

"Oggi abbiamo a che fare con la criminalità informatica organizzata e con i suoi forum di vendita che riuniscono diversi profili: quelli che individuano le vulnerabilità, quelli che si introducono nei sistemi, quelli che sviluppano il malware, ecc. Questi canali permettono inoltre di reclutare gli operatori per portare a termine l'intrusione. "

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

INFO CHIAVE

PROFILI JUNIOR

Il franchise ransomware Conti forma quindi profili "junior", offrendo loro uno stipendio fisso e un sistema di partecipazione agli utili.

PANORAMICA DEI GRUPPI DI RANSOMWARE

Il co-fondatore di Hackers Without Borders, Clement Domingo, ha identificato poco più della metà dei gruppi di cybercriminali presenti nel mondo.

- → ALPHV
- → Ako
- → Arvin Club
- → Astro Team
- → AtomSilo
- → Avaddon
- → AvosLocker
- → Babuk
- → Babuk Locker
- → Bl4ckt0r
- → Black Shadow
- → BlackByte
- → Bonaci Group
- → CRYP70N1C0D3
- → Clop
- → Conti
- → Cuba
- → DarkLeaks
- → DarkSide
- → DoppelPaymer
- → Dotadmin
- → Egregor
- → Entropy
- → Everest
- → Exorcist
- → Grief
- → HARON
- → Hive
- → LV
- → LockBit
- → LockBit 2.0
- → LockData Auction
- → Lorenz
- → Maze
- → Medusa Locker
- → Midas
- → Mount Locker
- → Nefilim
- → Nemty
- → NetWalker
- → Night Sky
- → Pay2Key
- → payload.bin
- → Prometeus
- → Pysa (Mespinoza)
- → Qlocker
- → Quantum
- → REvil (Sodinokibi)
- → Ragnar Locker
- → Ramp
- → Ransom Cartel
- → RansomEXX
- → Ranzy Locker
- → Rook
- → Sekmet
- → Snatch
- → SunCrypt
- → Suncrypt
- → Vice Society
- → Xing

NUOVE COMPETENZE… SU ENTRAMBI I FRONTI!



INTERVISTA **FLORENT CURTET**
— EX HACKER RICONVERTITO NELLA LOTTA ALLA CYBERCRISI, FORMATORE PRESSO FORZE DELL'ORDINE, STUDI LEGALI O DPO IN QUESTA NUOVA ARTE DEL NEGOZIATO

→ Gli attori del ransomware si stanno specializzando: sviluppo, aggiornamento, scambio con le vittime, riciclaggio di denaro virtuale, ognuno con il proprio ruolo nell'era del RaaS e dell'affiliazione. Anche sul fronte della sicurezza stanno emergendo nuove competenze, come dimostra la carriera atipica di Florent Curtet, direttore di NeoCyber e cofondatore di Hackers Without Borders.

Qual è stato il suo più grande successo in materia di negoziazione?

F.C. - I miei metodi hanno permesso di ridurre drasticamente l'importo del riscatto, da 1 milione di euro a 100.000 euro, ad esempio. Mi è capitato di convincere i cybercriminali a rinunciare al loro bottino in un contesto molto specifico come quello del settore sanitario.

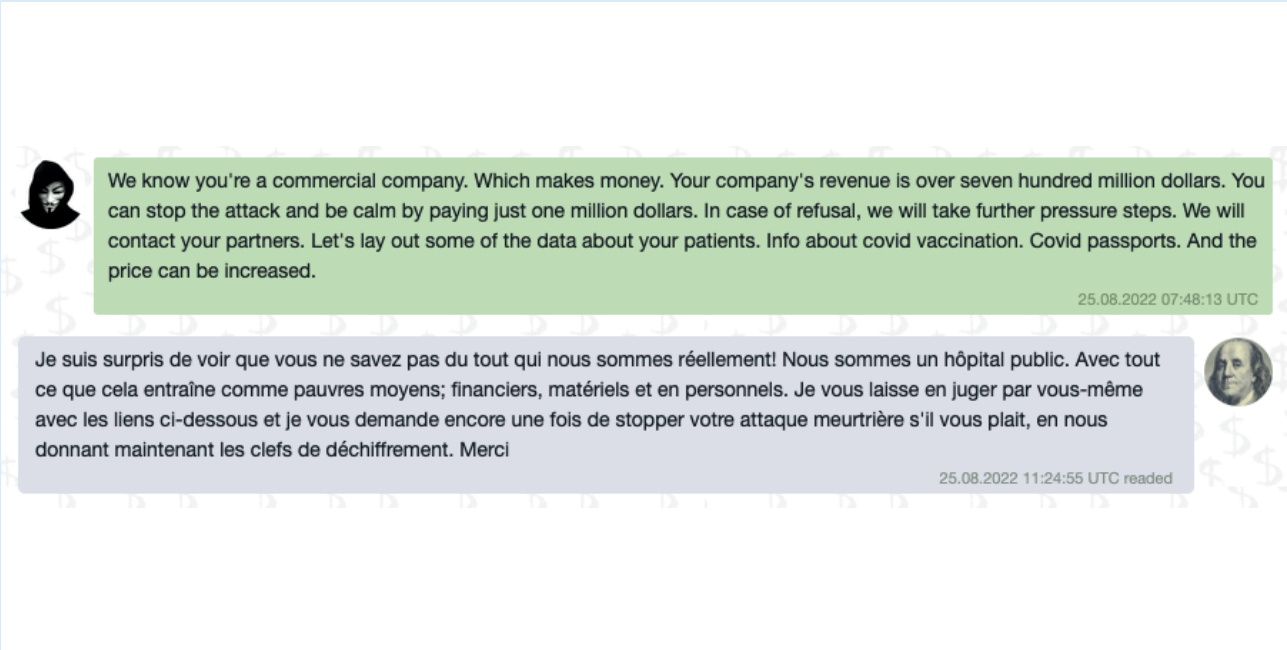
Quali sono i suoi metodi?

F.C. - Inizialmente, la sfida risiede negli strumenti di comunicazione. In generale, i criminali informatici contattano le loro vittime tramite e-mail. Il mio obiettivo è spostare la conversazione sul sistema di messaggistica in tempo reale Tox per stabilire un contatto più stretto. In questo modo è possibile tenerli occupati per guadagnare tempo, mostrare loro che siamo presenti e iniziare a entrare nel loro cervello.

Qual è il profilo dei criminali informatici con cui avete a che fare?

F.C. - Anche se spesso sono guidati da persone più esperte, si tratta in genere di profili ancora piuttosto giovani e influenzabili.

"Ho avuto l'impressione che ci fosse bisogno di formazione da entrambe le parti. "



LEGENDA

Nel caso specifico dell'attacco CHSF, il cybercriminale è convinto di avere a che fare con un'impresa commerciale[14].

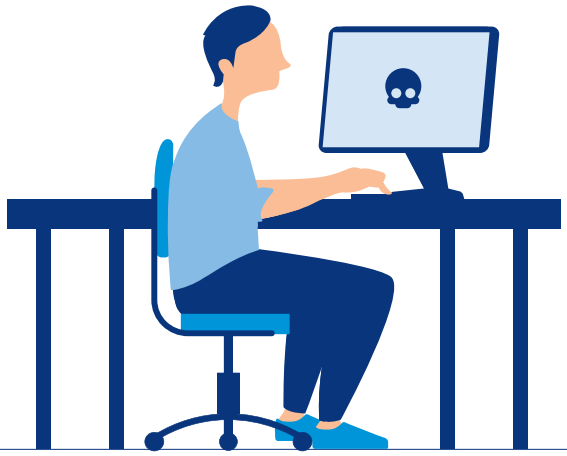
Il ruolo del negoziatore può sembrare ambiguo, soprattutto in un contesto in cui l'ANSSI sconsiglia vivamente di pagare un riscatto in caso di attacco ransomware. Perché ha scelto di sviluppare questa competenza?

F.C. - Ho avuto l'impressione che ci fosse bisogno di formazione da entrambe le parti. Storicamente, la negoziazione informatica è servita principalmente a spiegare all'azienda vittima cos'è il bitcoin, cos'è la rete Tor, ecc. Quando parlavo con i cybercriminali, a volte mi ritrovavo a spiegare la differenza tra fatturato e profitto o a ridefinire l'attività dell'azienda.
In effetti, ci si può trovare rapidamente in una zona grigia, per cui è importante regolamentare questa attività per evitare abusi. Tuttavia, la negoziazione a mio avviso è una risposta pragmatica in un contesto dove alcune piccole realtà rischiano una triplice sanzione: il blocco delle attività, la divulgazione dei dati e persino una potenziale multa da parte del Garante della privacy in caso di non conformità al GDPR. —

"Ci si può trovare rapidamente in una zona grigia, per cui è importante regolamentare questa attività per evitare abusi. "

2.2 Chi sono le vittime?

Il ransomware ha dimostrato la sua capacità di compromettere qualsiasi azienda o comunità, indipendentemente dalle sue dimensioni o dal livello di protezione. Ma ci sono profili o settori particolarmente sensibili? Analizziamo alcune risposte in merito.



L'intero tessuto economico globale è colpito dalla minaccia del ransomware: dalle microimprese alle grandi aziende internazionali. In Europa, un'azienda su due che cade vittima di ransomware è una microimpresa-PMI[15]. In paesi come la Francia, una PMI su tre ha già subito un attacco di questo tipo[16]. Ma questa è solo la punta dell'iceberg: quanti ransomware non dichiarati ci sono per ognuno di quelli dichiarati?

E sono coinvolti tutti i settori. Anche se in alcuni periodi il volume degli attacchi è ridotto, in genere sono più indirizzati e concentrati su alcuni settori, in particolare quello manifatturiero, tecnologico e finanziario[17].
Quando non sono direttamente prese di mira, le aziende possono anche subire danni collaterali da attacchi ransomware ai loro fornitori di servizi. —

11 m$[18]

"Nessuno è al sicuro dai cybercriminali, che praticano sia la "pesca a strascico" (attacchi di massa a strutture poco protette per interromperne l'attività) sia la "pesca a canna" (azioni mirate per attaccare l'immagine del marchio o il know-how industriale di soggetti più tutelati)".

FLORENT CURTET — DIRETTORE DI NEOCYBER E COFONDATORE DI HACKERS WITHOUT BORDERS

CIFRE SALIENTI

È l'importo versato dal colosso alimentare brasiliano JBS[19], paralizzato nel 2021 da un attacco ransomware del gruppo REvil.

I SETTORI PIÙ COLPITI DAL RANSOMWARE NEL 2022



Fonte Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

2.3 Quali sono gli effetti sulle strutture coinvolte?

Oltre alla perdita di dati, le aziende vittime devono affrontare altre conseguenze potenzialmente destinate a durare nel tempo: interruzione della produzione, calo del fatturato, rischi legali, perdita di fiducia da parte dei clienti, ecc.



Da 2 a 3 miliardi di euro

Come suggerisce il nome, la conseguenza logica di un attacco ransomware è la richiesta di un riscatto. Ma le ripercussioni per le vittime non si limitano a questo. Nella maggior parte dei casi, si troveranno a subire un'interruzione o addirittura un blocco della produzione che comporteranno a loro volta una perdita di fatturato o, nei casi più estremi, la chiusura dell'azienda.

Tutto ciò senza risparmiare i dati, che possono rischiare di essere divulgati, danneggiati o addirittura distrutti. In ogni caso, quando i cybercriminali accedono ai dati, espongono le aziende vittime a rischi legali in caso di accertata violazione del GDPR. Infine, la reputazione di un'azienda viene spesso compromessa da un attacco ransomware.

Tra le conseguenze più indirette, i ricercatori[20] hanno evidenziato che la pressione esercitata sui professionisti della sicurezza informatica in seguito alle minacce di ransomware sta contribuendo all'aumento del turnover all'interno di questi team. —

CIFRE SALIENTI

È il costo stimato dell'attacco ransomware che ha colpito Clestra Hauserman nell'aprile 2022. Il produttore alsaziano di pareti divisorie per uffici e "camere bianche", già in difficoltà a causa dell'attuale situazione economica e geopolitica, è stato posto in amministrazione controllata[21] per un periodo di sei mesi.

+71%

CIFRE SALIENTI

RICHIESTE DI RISCATTO SEMPRE PIÙ ALTE...

500 dollari nel 2016, 300.000 dollari nel 2020, quasi 1 milione di dollari nei primi 5 mesi del 2022.

(ossia +71% rispetto al 2021).

PER APPROFONDIRE

EFFETTI PSICOLOGICI

La principale conseguenza di un cyber-attacco ransomware è ovviamente di natura finanziaria. Ma è davvero l'unica? Ciò significherebbe ignorare le dimensioni sociali e psicologiche (troppo) spesso trascurate degli attacchi.

2.4 Pagare o non pagare? Bisogna cedere?

Pagare o non pagare? Bisogna cedere o no di fronte a una richiesta di riscatto? Una questione spinosa che ha reso insonni molti decisori.
La decisione riguarda infatti la salute finanziaria della struttura, nonché la sua attività, ma anche questioni inerenti la reputazione e l'etica.



Quali sono le aziende che pagano il riscatto? Difficile rispondere, in quanto solo poche di esse lo ammettono. Decriptare piuttosto che ricostruire, o addirittura scomparire: le strutture più piccole non esiteranno a lungo, poiché la loro sopravvivenza può dipendere da questo... Le aziende più grandi cederanno soprattutto per motivi di reputazione o finanziari. Qualunque sia la ragione, pagare un riscatto rappresenta spesso l'ultima alternativa possibile. È inoltre importante ricordare che aver già subito un attacco ransomware non protegge da un nuovo tentativo. Ad esempio, un'azienda britannica[22] è stata costretta a pagare un riscatto per due volte a distanza di poche settimane l'una dall'altra.

CIFRE SALIENTI

L'80%

Circa l'80% delle aziende che pagano la richiesta di riscatto subisce in seguito un nuovo attacco[23].

In paesi come la Francia, il via libera concesso dal Ministero dell'Economia al risarcimento dei riscatti da parte degli assicuratori, subordinato alla presentazione di una denuncia, potrebbe avere effetti controversi, oltre a offuscare il messaggio dell'autorità nazionale in materia, l'ANSSI[24].

—

"Il testo ha il merito di esistere e di far parlare di sé nelle alte sfere, ma non cambierà il problema di fondo. Tra gli aspetti positivi c'è il fatto che dovrebbe porre fine alle attività di ransomware "sottobanco" per evitare potenziali sanzioni da parte del Garante della privacy.[25]"

SÉBASTIEN VIOU — DIRETTORE DELLA SICUREZZA INFORMATICA E CYBER-EVANGELISTA

PODCAST

RANSOMWARE: È OPPORTUNO

Per affrontare una questione così spinosa, cosa c'è di meglio di un podcast tra esperti? Una discussione sulle opportunità offerte da questo progetto legislativo con Valéry Rieß-Marchive, caporedattore di MagIT, Fabrice Epelboin, Damien Douani e Bertrand Lenotre.

ULTIME NOTIZIE

RISARCIMENTO PER LE AZIENDE COLPITE DA RANSOMWARE: IL DELICATO TEMA DELLA CYBER-ASSICURAZIONE



Tutto è iniziato in Francia nel giugno 2021. Bruno Le Maire, Ministro dell'economia, delle finanze e della sovranità industriale e digitale e la Direzione Generale del Tesoro hanno istituito un gruppo di lavoro sullo sviluppo di un'offerta assicurativa per la copertura dei rischi informatici, che riunisce dipartimenti governativi, rappresentanti delle imprese, società di assicurazione e riassicurazione ed esperti del mondo accademico.

È in corso di definizione un piano d'azione articolato su 4 assi:

- → **Chiarire il quadro giuridico per l'assicurazione contro i rischi informatici,**
- → **Comprendere e valutare al meglio il rischio informatico,**
- → **Migliorare la condivisione dei rischi tra assicurati, assicuratori e riassicurati,**
- → **Intensificare le iniziative di sensibilizzazione.**

Sulla base di questa relazione, il Ministero dell'Economia e delle Finanze sta proponendo al Consiglio dei Ministri, alla fine del 2022, una misura dedicata alla criminalità informatica all'interno del disegno di legge di orientamento e programmazione del Ministero dell'Interno (LOPMI). L'unica condizione è che l'azienda vittima presenti una denuncia entro 48 ore dalla scoperta dell'attacco informatico. Successivamente, il testo approvato dalla Commissione giuridica (nell'Assemblea nazionale) non includerà più la parola riscatto, ma utilizzerà una terminologia più ampia per indicare i danni causati da un attacco informatico.

Con la pubblicazione di queste notizie si sono levate molte voci che hanno messo in evidenza una serie di rischi e di incognite legate a tale approccio. Incognite riguardanti il riscatto stesso: chi pagherà? Direttamente l'azienda o un intermediario, come ad esempio un negoziatore? In che modo vanno supervisionati? Qual è l'importo del rimborso? E le possibili conseguenze: l'ammontare dei riscatti aumenterà? Le aziende europee saranno prese maggiormente di mira? Sebbene sia ancora troppo presto per rispondere a queste domande, in futuro sono destinate a rivestire un ruolo centrale.

Mentre altri sottolineano un risvolto positivo nel pagamento dei riscatti (come un migliore esame dei flussi finanziari, da cui possono scaturire indizi per rintracciare i criminali informatici), il dibattito rimane più che mai aperto. —

INTERVISTA

RISCATTO: PAGARE O NON PAGARE? LA DOMANDA È ANCORA ATTUALE?

a **La raccomandazione ufficiale dell'ANSSI è inequivocabile: non bisogna pagare il riscatto richiesto. Tuttavia, in Europa, nel 2021, un'azienda attaccata su cinque si è arresa. Perché?**

PERCHÉ NON BISOGNA PAGARE IL RISCATTO?

"Molte aziende ritengono che questo sia il modo migliore per ripristinare le attività nel più breve tempo possibile. Ma non è detto che sia così. Spesso, lo strumento di decriptazione progettato dall'aggressore presenta dei bug. Inoltre, la mancanza di fiducia richiede una fase di analisi prima del ripristino dei dati. Va ricordato che il ripristino dei dati resta il metodo più sicuro per recuperarli: in media, solo il 54% delle aziende che pagano riesce a recuperarli. "[28]

ARNAUD PILON —
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

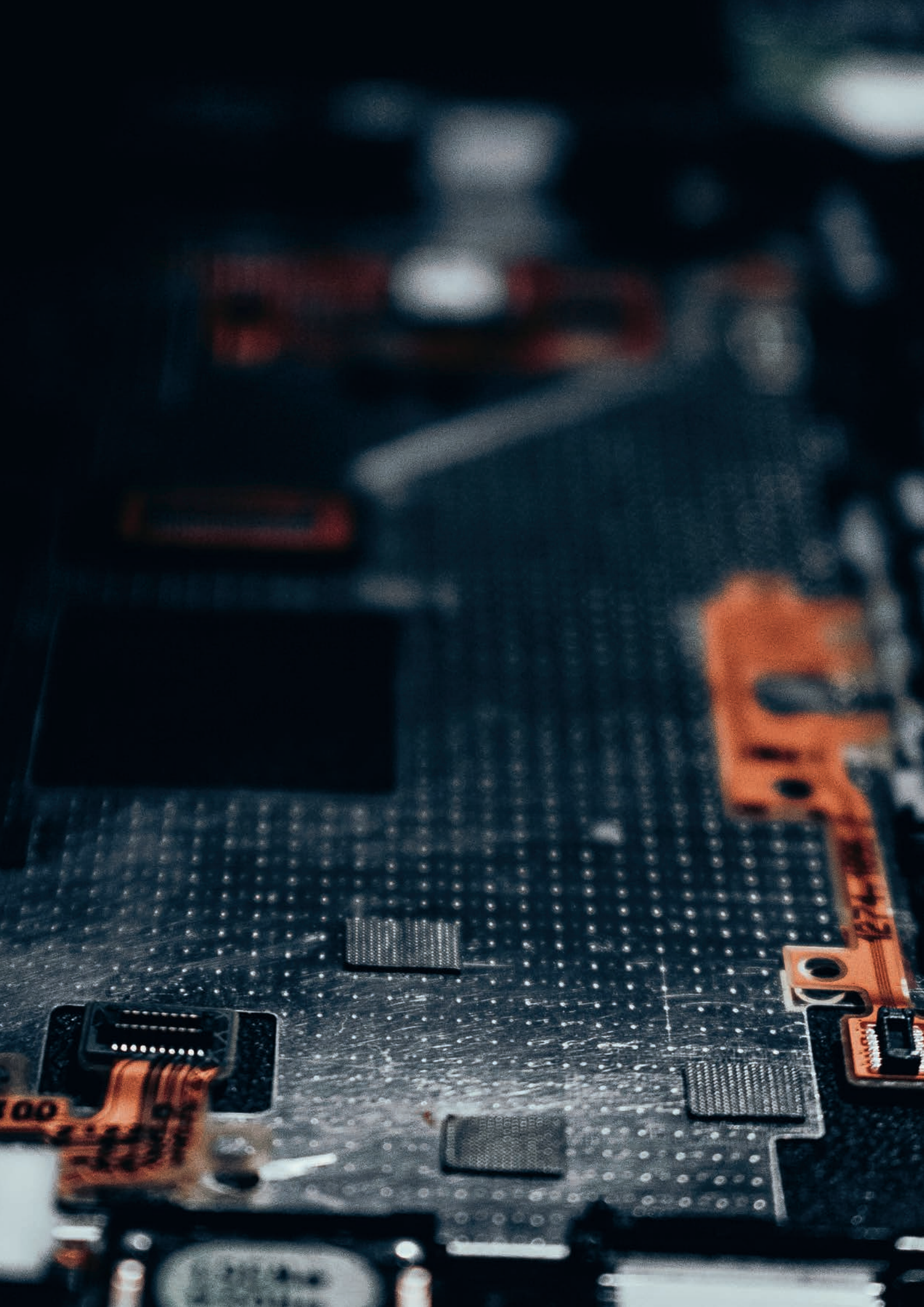
"Da un punto di vista etico, il pagamento può essere visto anche come un'approvazione del modello. È qui che nasce la controversia sul modello di rischio degli assicuratori. "

NICOLAS CAPRONI —
HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

PERCHÉ ALCUNE AZIENDE NON HANNO SCELTA?

"Le vittime sono talvolta aziende molto giovani che non hanno ancora potuto investire nel backup dei propri dati. In questo caso, il pagamento è una questione di sopravvivenza. Invece di condannare queste strutture messe alle strette, le autorità potrebbero utilizzare la tracciabilità dei pagamenti per sgominare le bande di ransomware e provvedere parallelamente allo sviluppo di una sorta di controllo tecnico cibernetico. Perché non introdurre un credito d'imposta per le verifiche di sicurezza delle start-up? "

FLORENT CURTET —
DIRETTORE DI NEOCYBER E COFONDATORE
DI HACKERS WITHOUT BORDERS



Come funziona un ransomware: la meccanica dei fluidi

Sono diversi i terminali che possono essere presi di mira dal ransomware: una postazione di lavoro, un telefono cellulare, un macchinario in una fabbrica, una bicicletta connessa in una palestra, ecc.

3.1 Itinerario del ransomware

Come si diffonde il ransomware? Quali sono i suoi principali elementi conduttori? Accesso iniziale e infezione, camuffamento, ricerca di vulnerabilità sfruttabili... Il processo prevede diverse fasi strategiche e ben collaudate.



Storicamente, il termine "ransomware" è stato utilizzato per indicare principalmente i "blocker" che bloccavano l'accesso al sistema e i "crypto" che criptavano i dati.

Oggi si applica a tutti i programmi che consentono l'estorsione. Si tratta di un tipo di attacco complesso che si basa su diversi meccanismi e ambiti temporali. Tuttavia, questi attacchi partono sempre da un'infezione iniziale, che può avvenire tramite phishing, download peer-to-peer, download drive-by, sfruttamento di una vulnerabilità, ecc.

A questa fase segue quella dell'attacco vero e proprio, durante la quale il "dropper" crea una backdoor sul sistema che consentirà l'installazione di tutti gli strumenti necessari per l'attacco, aggirando i meccanismi di rilevamento, prima che il "loader" ne garantisca la corretta esecuzione.

Successivamente, il criminale informatico entra nella fase di Evasione della Difesa, durante la quale cercherà di coprire le tracce della sua intrusione in modo che la backdoor sopravviva al riavvio. La fase seguente, quella di *Accesso alle credenziali*, consiste nell'ottenere l'accesso sottraendo nomi di account e password. Segue poi un periodo che va da poche ore a qualche mese (*Discovery* o "rilevamento della rete"), durante il quale i criminali informatici cercano punti di ingresso per espandersi lateralmente. Questi punti di accesso possono consistere in password rubate, vulnerabilità sfruttabili o impostazioni di sicurezza errate. A questo punto individuano i file che contengono dati di valore (*Raccolta*) e li criptano, a volte esfiltrandoli prima ed eliminando i backup.

Il passo finale consiste nel fare pressione sulla vittima pubblicando le prove dell'attacco, ad esempio gli screenshot sul sito web della banda criminale, di solito sulla rete Tor. A volte i cybercriminali effettuano parallelamente anche un attacco di tipo denial of service. Si tratta di un'ulteriore sollecitazione per spingere la vittima a pagare più rapidamente e anche per impedire all'azienda di comunicare, ad esempio, sul proprio sito web. —

PAROLA CHIAVE

Il "dropper" è un programma informatico progettato per installare software dannosi in un sistema. Il "loader" si occupa di garantirne l'esecuzione.

Dropper

COME SPIEGARE IN MODO SEMPLICE IL MECCANISMO DEL RANSOMWARE?

ACCESSO INIZIALE
↓
ESECUZIONE
INTERFACCIA A RIGA DI COMANDO
↓
PERSISTENZA
↓
ESCALATION DEI PRIVILEGI
↓
ELUSIONE DELLA DIFESA
FILE HTML COMPILATI
↓
CREDENZIALI D'ACCESSO
CHIAVI PRIVATE
↓
RILEVAMENTO
RILEVAMENTO DEI PROCESSI
↓
SPOSTAMENTO LATERALE
↓
RACCOLTA
DATI DAL SISTEMA LOCALE
↓
COMANDO E CONTROLLO
↓
ESFILTRAZIONE
DATI COMPRESSI
↓
IMPATTO
DATI CRITTOGRAFATI PER L'IMPATTO

Fonte: framework MITRE ATT&CK

3.2 Focus sull'accesso iniziale

Una volta individuata la vittima, il cybercriminale dà inizio al minuzioso lavoro di penetrazione nel sistema informatico aziendale. Alla ricerca di un passpartout: i famosi accessi iniziali.





Una volta individuata la vittima, il cybercriminale dà inizio al minuzioso lavoro di penetrazione nel sistema informatico aziendale. Alla ricerca di un passpartout: i famosi accessi iniziali.

Questi accessi costituiscono la chiave di volta dei gruppi di ransomware, in quanto vengono utilizzati per introdursi nel sistema informatico delle loro potenziali vittime. Per questo motivo richiedono una lunga fase di ricognizione. " *L'analisi dei bersagli va al di là del semplice studio tecnico della della superficie di attacco esposta in Internet,* spiega Valéry Marchive in un articolo[29] pubblicato su Le Mag IT. *Questa operazione prevede l'ottenimento dei dati di contatto di ogni persona individuata, Probabilmente per fare pressione dopo il lancio del ransomware.* "

Per recuperare tutti questi dati, vengono impiegate diverse tecniche. Le e-mail di phishing, **con vari gradi di sofisticazione** costituiscono il vettore classico per eccellenza. Allo stesso tempo, vengono utilizzati anche altri canali per implementare tecniche di ingegneria sociale simili, come la messaggistica di LinkedIn.

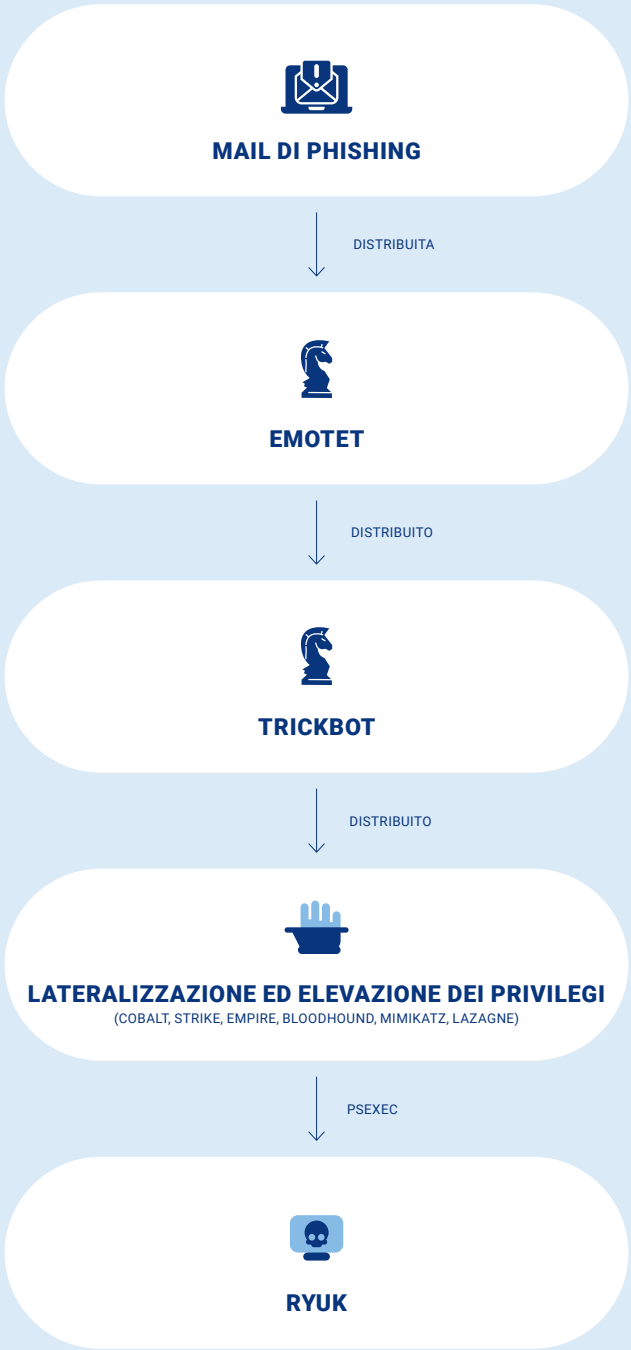
PER APPROFONDIRE

RANSOMWARE: ECCO COME I CONTI PREPARANO I LORO ATTACCHI INFORMATICI.

Un articolo che illustra come il Gruppo Conti stia ottenendo l'accesso iniziale ai sistemi informatici di diverse aziende in tutto il mondo.

IL RANSOMWARE SI INSERISCE A SUA VOLTA IN UNA CATENA PIÙ COMPLESSA

FLUSSO SEMPLIFICATO DELLA CATENA DI INFEZIONE EMOTET-TRICKBOT-RYUK



Fonte Report “Il ransomware Ryuk”, ANSSI, 2021

Tuttavia, anche il software utilizzato nelle aziende può costituire una superficie di attacco se contiene inconsapevolmente una vulnerabilità, spesso sfruttata durante la fase di replica.

"Non è raro che i cybercriminali utilizzino altri malware come Emotet, Trickbot o il loader Bumblebee per portare a termine il loro attacco. "

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

"Le tecnologie sono diventate interoperabili. In questo caso, Emotet agisce come un cavallo di Troia, recupera il codice reso disponibile dall'aggressore e si propaga come un worm. Si tratta dunque di un mezzo piuttosto che di un fine. Trickbot, per contro, è una botnet che si infiltra nel client, attende istruzioni da Emotet e le esegue. "

PIERRE-OLIVIER KAPLAN — INGEGNERE DI RICERCA E SVILUPPO, STORMSHIELD

Un altro fattore che rende gli attacchi più complessi è la proliferazione attraverso la catena di approvvigionamento: i criminali informatici compromettono intere catene di approvvigionamento prendendo di mira le vulnerabilità nei software aziendali e/o nei servizi cloud. Nel maggio 2021, il fornitore di soluzioni IT Kaseya è stato attaccato da REvil. Attraverso le reti di 60 clienti, sono state colpite più di 1.500 aziende e il riscatto richiesto ammontava a 70 milioni di dollari[30]. —

+1500

CIFRE SALIENTI

In seguito a un'infezione del software di Kaseya sono state colpite più di 1.500 aziende


SYSTEM
HACKED

Quali sono le strategie da mettere in atto per smantellare questo meccanismo fraudolento?

Il ransomware è diventato il flagello dei reparti IT e delle aziende in generale. Ma è inevitabile? Abbiamo chiesto a Sébastien Viou, direttore della sicurezza informatica dei prodotti e cyberevangelista di Stormshield, quali misure adottare per far fronte alla situazione.

01

PROTEGGERSI PRIMA DI UN ATTACCO RANSOMWARE

ESEGUIRE IL BACKUP DEI DATI… E PROTEGGERLO[31]
"Questa precauzione da sola non è sufficiente, perché è la prima cosa che il ransomware cercherà di distruggere, prima ancora della crittografia. È necessario ricorrere a backup su nastro disconnessi dalla rete e stabilirne la frequenza. Occorre inoltre testare i ripristini per accertarsi che i backup siano utilizzabili. ".

MANTENERE AGGIORNATI SOFTWARE E SISTEMI
"Gli aggiornamenti devono essere eseguiti costantemente e devono riguardare i PC Windows, ma anche i sistemi Linux e Mac, che possono costituire dei punti di accesso. È coinvolto l'intero parco informatico aziendale: da Microsoft Exchange ad Active Directory e tutti i server esposti, anche quelli di piccole dimensioni. ".

PARTIZIONE DEL SISTEMA INFORMATICO
"Si raccomanda di applicare regole rigorose sui flussi consentiti tra le diverse aree in base alla loro criticità. "

LIMITARE I DIRITTI DEGLI UTENTI

E LE AUTORIZZAZIONI DELLE APPLICAZIONI
"Su questo punto, è la gestione nel tempo a essere decisiva: per garantire la sicurezza, è necessario pianificare controlli regolari. "

IMPLEMENTARE IL MONITORAGGIO DEI LOG
"La raccolta dei log rappresenta un obbligo. Nei casi in cui è richiesto un livello di sicurezza molto elevato, è possibile aggiungere un componente di rilevamento delle intrusioni tramite un SOC. "

SENSIBILIZZARE I COLLABORATORI
"Con l'ingegneria sociale, la principale porta d'accesso al sistema informatico di un'azienda è costituita dal suo personale. È quindi fondamentale affrontare i temi della cybersicurezza, anche se la sensibilizzazione ha i suoi limiti. "

L'8%

è la percentuale di dipendenti del CERN ingannati da una falsa campagna di phishing, implementata in seguito a un'attività di sensibilizzazione.[32]

ELABORARE UNA PROPRIA STRATEGIA DI COMUNICAZIONE PER LE CRISI INFORMATICHE
"Anche in questo caso, è utile aver definito in anticipo i messaggi e i contatti da utilizzare per comunicare in modo adeguato con i diversi tipi di destinatari. Tali comunicazioni servono ad avvertire, ad esempio, di interruzioni impreviste della produzione o di fughe di dati personali, come richiesto dal GDPR. "

IMPLEMENTARE UN PIANO DI RISPOSTA AGLI ATTACCHI INFORMATICI
"Questo piano è fondamentale, perché ci permette di reagire rapidamente, ad esempio contattando le organizzazioni CERT identificate in anticipo. Ovviamente include una componente tecnica, con l'implementazione di soluzioni di protezione come Stormshield Endpoint Security Evolution e Stormshield Network Security. "

VALUTARE LE OPPORTUNITÀ DI SOTTOSCRIVERE UN'ASSICURAZIONE CONTRO LE MINACCE INFORMATICHE
"Alcune polizze di cyber-assicurazione includono clausole sull'implementazione di soluzioni di sicurezza informatica; da questo punto di vista sono interessanti, perché impongono una certa protezione. Tuttavia, la cyber-assicurazione non dovrebbe essere vista come una misura di salvaguardia a sé stante, e ancor meno come una misura di protezione. In altre parole, l'assicurazione contro il ransomware non sarà mai una strategia di sicurezza informatica. "

02

LIMITARE I DANNI DURANTE UN ATTACCO RANSOMWARE

- **AVERE DEI BUONI RIFLESSI**
  "Bisogna essere in grado di accorgersi rapidamente che qualcosa non va e non esitare a scollegare tutto per mitigare il rischio e contenere il più possibile la diffusione". Anche a livello individuale dobbiamo imparare a reagire, a dire "ho cliccato nel punto sbagliato", perché ogni minuto è importante. "
- **AFFIDARE LA GESTIONE DELLA CRISI INFORMATICA AL COMITATO ESECUTIVO**
- **COMUNICARE AL GIUSTO LIVELLO**
- **PRESENTARE UNA DENUNCI**

03

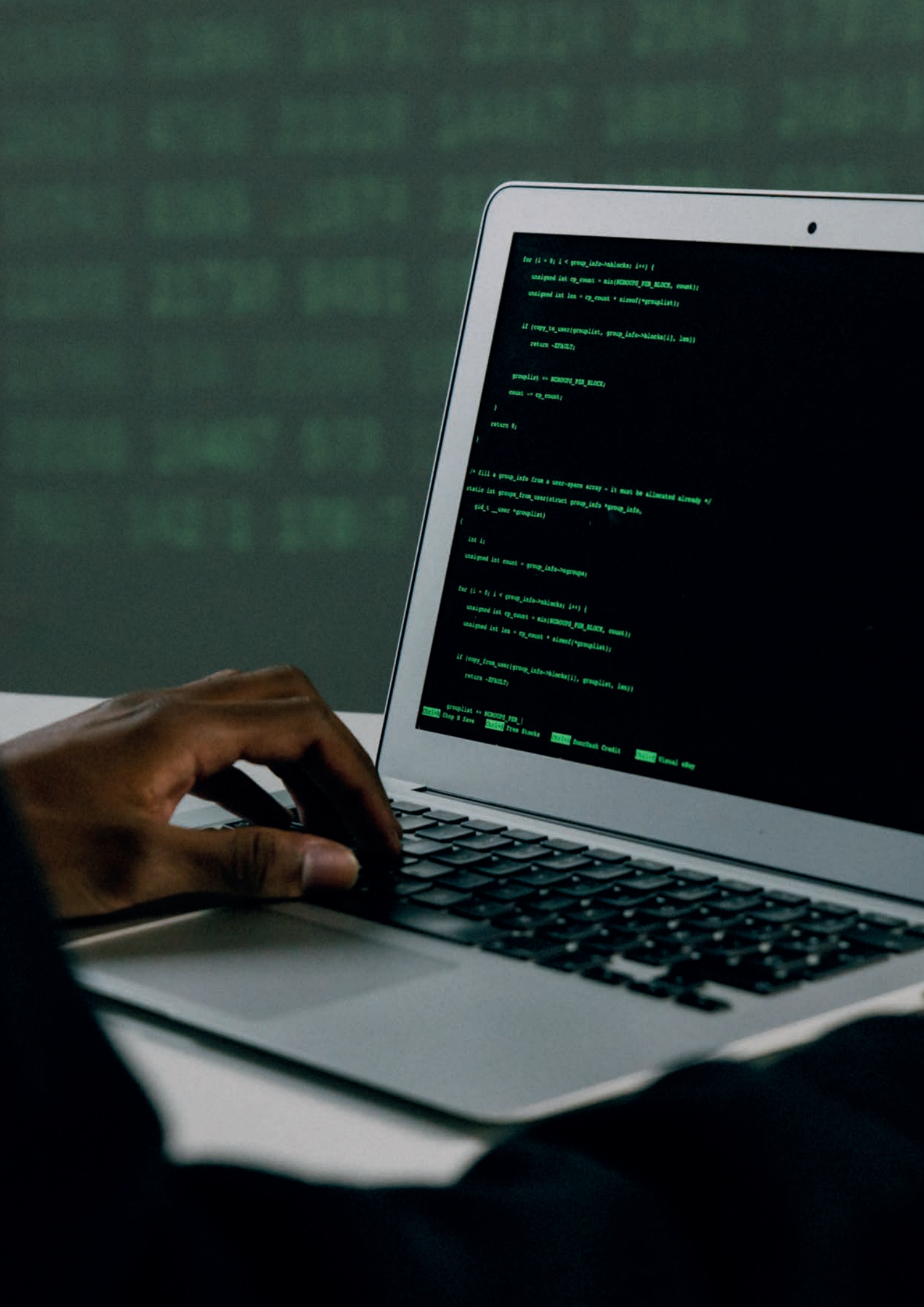
RIPRENDERSI DA UN ATTACCO RANSOMWARE

- **RIPRISTINARE I SISTEMI DA SORGENTI SANE**
- **INDAGARE IL PERCORSO DI ATTACCO**
  "Per valutare l'andamento dell'attacco e le debolezze del proprio sistema, bisogna analizzare ciò che è successo. Solo in questo modo potremo evitare che ciò accada di nuovo. "
- **ELABORARE UN PIANO CORRETTIVO**
  "A seconda dei casi, potrebbe rendersi necessario impostare un'autenticazione multifattore o migliorare le soluzioni di sicurezza presenti sulle postazioni di lavoro? "
- **INOLTRARE LA PRATICA ALLA COMPAGNIA DI ASSICURAZIONE**
- **DIFFONDERE IL PIANO DI COMUNICAZIONE AI CLIENTI INTERESSATI, AI PROPRI INVESTITORI, ECC.**
- **GESTIRE L'IMPATTO PSICOLOGICO SUI DIPENDENTI**
  "Cassa integrazione, sensi di colpa, team IT sovraccarichi di lavoro: il ransomware determina conseguenze anche per le risorse umane, da tenere in considerazione". "
- **INTRAPRENDERE UN'AZIONE LEGALE, SE NON È GIÀ STATA AVVIATA.**
- **STABILIRE UN PIANO DI PRODUZIONE PER RECUPERARE IL RITARDO ACCUMULATO**

COSA PREVEDE STORMSHIELD ENDPOINT SECURITY EVOLUTION PER FRONTEGGIARE

→ SES Evolution offre una serie di funzionalità particolarmente utili nella lotta contro la minaccia del ransomware: rilevamento della crittografia dei file, protezione dei backup automatici e da infiltrazioni di DLL, analisi comportamentale e blocco in tempo reale dei processi anomali. —

PER SAPERNE DI PIÙ, GUARDARE IL VIDEO



Che futuro si prospetta per il ransomware?

Cosa succederà al ransomware in futuro? Punterà sui portafogli di criptovalute? Sui veicoli autonomi? I cybercriminali utilizzeranno l'intelligenza artificiale per effettuare attacchi polimorfi? No, non siamo in una distopia. È semplicemente il mondo in cui viviamo.

5.1 Quali caratteristiche avrà il ransomware di domani?

Il profilo del ransomware di domani non è ancora stato delineato. Ma una cosa è certa: diventerà più complesso e si adatterà a un ambiente maggiormente sicuro.
Inoltre, si rivolgerà ad aziende più mature e a contesti geopolitici fragili.



Sebbene LockBit sia attualmente il franchise di ransomware più popolare, la concorrenza è agguerrita. Nella sola prima metà del 2022 sono spuntate venti nuove bande. La situazione geopolitica e le imminenti

"Possiamo immaginare che domani questi ransomware vadano a colpire portafogli di criptovalute, NFT e veicoli a guida autonoma. Le tecnologie emergenti non ne sono immuni. "

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

crisi economiche sono un terreno fertile per i ransomware. I loro autori stanno raddoppiando gli investimenti in ricerca e sviluppo.
Tuttavia, tali sviluppi sono ancora piuttosto

"Le nostre indagini tecniche hanno inoltre rivelato che un gruppo RaaS a doppia estorsione poco conosciuto, chiamato Vice Society, utilizza ransomware diversi a seconda dei bersagli e dei sistemi: Zepplin per Windows, HelloKitty per Linux.[33]"

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

costosi e costringono i cybercriminali a prendere di mira le grandi aziende per ammortizzare le spese. —

NUOVE FAMIGLIE DI RANSOMWARE NEL 1° SEMESTRE 2022

- → YourCyanide
- → Vandili
- → GoodWill
- → Vulcan Ransom Team
- → Cheerscrypt
- → NwGen
- → Axxes
- → RTM
- → Nokoyawa
- → Pandora
- → Hermetic Ransom
- → Mindware
- → Yashma
- → Onyx
- → Black Basta

Fonte Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

COME LOCALIZZARE UN RANSOMWARE?

CON **ARNAUD PILON** — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ "Tenere il passo con il ransomware non è facile". Stiamo cercando di individuare invarianze nei metodi operativi, nelle tecniche e negli strumenti, poiché non è insolito che gruppi diversi condividano "espedienti", ad esempio sui metodi di propagazione. Teniamo d'occhio anche le campagne di phishing, che non vanno sottovalutate. Infine, cerchiamo di determinare quali vulnerabilità sono suscettibili ad essere sfruttate in massa. » —

5.2 Quali soluzioni attendersi?

Di fronte a una minaccia in costante evoluzione, le soluzioni di protezione delle workstation devono tenere il passo. Il miglioramento e la moltiplicazione dei mezzi di rilevamento è una strada da esplorare, ma questo non deve farci dimenticare le necessarie soluzioni di protezione.



Il ransomware ha fatto in modo che si parlasse delle minacce ai sistemi informatici. Questa divulgazione ha risvegliato i CIO, spingendoli ad aumentare i livelli di sicurezza. Oltre a indurre i sistemi informatici a essere più robusti, la pressione del ransomware ha portato a una rinascita dell'industria dei backup.

Ad esempio, il mercato delle soluzioni di cybersicurezza offre già una serie di strumenti come EDR o XDR che potenziano gli strumenti di rilevamento e blocco del ransomware. Tuttavia, non bisogna dimenticare che queste soluzioni di rilevamento e correzione sono palliative: in questa fase, l'attacco informatico ha già causato danni alle aziende. **Il primo passo fondamentale è l'adozione di misure protettive** (per i dati, le postazioni di lavoro e le reti). L'orchestrazione delle soluzioni rappresenta quindi uno dei possibili interventi per ridurre l'affaticamento del SOC.

La sicurezza conferita dalle soluzioni implementate diventerà ancora più strategica di quanto non lo sia oggi. Ciò dovrebbe consolidare l'importanza dello schema di qualificazione a livello europeo e/o nazionale. —

"La sfida per i prossimi anni consisterà nel ridurre il numero di falsi positivi nei sistemi informatici su larga scala attraverso l'apprendimento automatico, ma non è un obiettivo fine a se stesso. D'altra parte, con la stratificazione dei prodotti destinati alla sicurezza, sarà fondamentale migliorare l'interoperabilità dei sistemi. "

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

AVREMO MAI UN "VACCINO" CONTRO IL RANSOMWARE?

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ ***"Purtroppo le minacce si adattano rapidamente a questo tipo di soluzione tecnica. Finché questi attacchi frutteranno denaro, i cybercriminali continueranno ad adattarsi, a investire in ricerca e sviluppo e quindi a progredire. "***

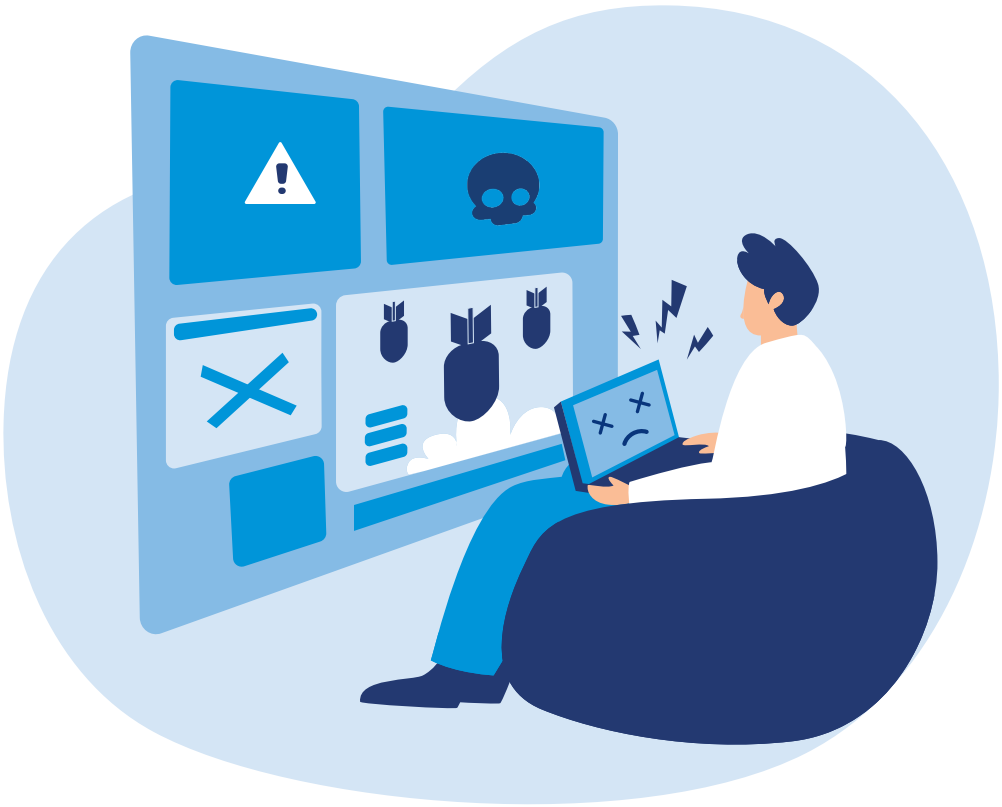
NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

→ ***"Non credo nei vaccini, ma nemmeno nella fatalità. La tipologia delle vittime dimostra che la maggior parte degli attacchi sono opportunistici. Naturalmente qualcuno cliccherà sempre su un allegato compromesso, ma con una combinazione di strumenti di rilevamento e consapevolezza delle minacce è possibile rilevare l'attacco prima della crittografia e***

FLORENT CURTET — DIRETTORE DI NEOCYBER E COFONDATORE DI HACKERS WITHOUT BORDERS

→ ***"Non esistono soluzioni a medio termine per arginare il fenomeno, soprattutto perché il modello di business dei ransomware continua a evolversi: alcuni utilizzano vulnerabilità molto avanzate e pagano gli "insiders" per eseguire il virus". "***

In definitiva, l'intelligence e la vittimologia sono fondamentali nella lotta contro il ransomware, in quanto consentono una migliore comprensione delle organizzazioni cybercriminali e quindi una migliore lotta contro tale minaccia. Ricordiamo che tale situazione è cambiata solo negli ultimi tre decenni. È quindi prevedibile che si continuerà a scoprire regolarmente nuovi ceppi e varianti, soprattutto nell'attuale contesto di tecnologie emergenti e conflitti geopolitici.



FONTI E ALLEGATI

[1] https://www.liberation.fr/futurs/2017/06/28/notpetya-le-logiciel-ranconneur-a-propagations-multiples_1580043/
[2] https://www.leparisien.fr/high-tech/cyberattaque-les-centrales-nucleaires-francaises-sont-elles-en-securite-28-06-2017-7094979.php
[3] https://www.insurancebusinessmag.com/asia/news/cyber/ransomware-big-game-hunting-has-major-impact-on-insurers-189773.aspx
[4] https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
[5] https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
[6] https://www.zdnet.com/article/these-ransomware-attackers-sent-their-ransom-note-to-the-victims-printer/
[7] https://www.stormshield.com/fr/actus/petite-histoire-des-ransomwares/
[8] https://www.fbi.gov/news/testimony/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks
[9] https://www.zdnet.fr/actualites/le-groupe-de-ransomware-conti-ferme-son-site-vitrine-39943928.htm
[10] https://www-lemagit-fr.cdn.ampproject.org/c/s/www.lemagit.fr/actualites/252522126/Cyberattaques-Karakurt-fait-un-retour-en-fanfare?amp=1
[11] https://www.zdnet.fr/actualites/le-site-du-groupe-revil-donne-des-signes-de-vie-39940953.htm
[12] https://www.latribune.fr/technos-medias/informatique/qui-est-lockbit-3-0-le-cyber-ranconneur-de-la-poste-mobile-925065.html
[13] https://www.linkedin.com/posts/clementdomingo_cybersaezcuritaez-ransomwares-ransomgangs-activity-6985605220269441024-ZqLc
[14] https://www.lemagit.fr/actualites/252524255CHSF-lattaquant-ne-semble-pas-comprendre-que-cest-un-hopital-public
[15] https://www.ouest-france.fr/societe/cyberattaque/cyberattaques-voici-combien-les-entreprises-francaises-ont-perdu-depuis-janvier-482ff564-dfe7-11ec-b2a8-056c7579e285
[16] https://www.channelnews.fr/une-pme-francaise-sur-trois-a-deja-ete-victime-dun-ransomware-114729
[17] https://www.zdnet.com/article/ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
[18] https://www.lemondeinformatique.fr/actualites/lire-ransomware-jbs-debourse-11-m$-pour-recuperer-son-it-83225.html
[19] https://www.zdnet.fr/actualites/le-geant-de-l-agroalimentaire-jbs-vise-par-revil-39923901.htm
[20] https://www.lesechos.fr/pme-regions/grand-est/clestra-hauserman-demande-sa-mise-en-redressement-pour-trois-mois-1778519
https://www.lemoniteur.fr/article/clestra-place-en-redressement-judiciaire.2217432
[21] https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
[22] https://securite.developpez.com/actu/313967/Victime-d-un-ransomware-une-entreprise-paie-des-millions-aux-cybercriminels-pour-restaurer-ses-fichiers-L-entreprise-se-fait-attaquer-a-nouveau-par-le-meme-ransomware-et-paie-encore/
[23] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[24] https://www.usine-digitale.fr/article/ransomwares-rembourser-la-rancon-un-jeu-dangereux-que-les-assureurs-continuent-de-jouer-sous-conditions.N2038932
[25] https://www.linkedin.com/posts/s%C3%A9bastien-viou-b0806861_cybersaezcuritaez-ransomware-activity-6973284015197827073-dAGn?utm_source=share&utm_medium=member_desktop
[26] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[27] https://www.clubic.com/antivirus-securite-informatique/actualite-442272-cybersecurite-faut-il-assurer-les-victimes-de-ransomware-le-senat-dit-oui.html
[28] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf
[29] https://www.lemagit.fr/actualites/252501084/

Ransomware-ces-rancons-payees-qui-plaident-en-faveur-de-la-cyberassurance

[30] https://www.numerama.com/cyberguerre/738790-apres-deux-mois-dabsence-le-terrible-gang-revil-fait-un-retour-inattendu.html

[31] https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

[32] https://www.cio-online.com/actualites/lire-experience-de-faux-phishing-au-cern-8%C2%A0-de-compromission-14450.html

[33] https://feedback.sekoia.io/changelog/11222

https://www.lesechos.fr/finance-marches/banque-assurances/assurance-bercy-donne-son-feu-vert-a-lindemnisation-des-cyber-rancons-1786154

https://www.usine-digitale.fr/article/assurance-un-projet-de-loi-clarifie-le-cadre-de-l-indemnisation-des-rancons-en-cas-de-cyberattaque.N2041292

https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/

https://www.cap-com.org/actualit%C3%A9s/20h02-la-web-serie-des-hopitaux-lyonnais-sur-la-covid-19

https://www.stormshield.com/fr/actus/50-nuances-de-ransomwares/

https://www.stormshield.com/fr/actus/vers-une-nouvelle-economie-de-la-vulnerabilite/

https://www.stormshield.com/fr/zero-ransomware/

https://www.stormshield.com/fr/ressourcescenter/ask-ze-expert-ransomware-ne-payez-pas-les-rancons/

https://www.stormshield.com/wp-content/uploads/SES-FR-Ransomware-Infographics-202204.pdf

https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf

https://www.stormshield.com/fr/actus/quel-etat-des-lieux-des-ransomwares-en-2020/

https://www.stormshield.com/fr/actus/alerte-securite-snake-combattre-infection-avec-stormshield-endpoint-security/

https://www.stormshield.com/fr/actus/ransomware-robbinhood-pourquoi-baltimore-se-retrouve-sous-les-projecteurs/

https://www.stormshield.com/fr/actus/tour-dhorizon-des-ransomwares-les-plus-wtf-de-la-planete/

https://www.stormshield.com/fr/actus/les-pirates-seraient-ils-des-juillettistes/

https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

https://www.idc.com/getdoc.jsp?containerId=US48093721

https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true

https://www.zdnet.com/article/ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true

https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/

https://cyware.com/news/ransomware-sprawl-fbi-finds-over-100-variants-to-be-active-88f659f6

https://youtu.be/azdrKZzyWgg

https://www.nomoreransom.org/fr/decryption-tools.html

https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf

https://www.vadesecure.com/fr/blog/ransomware-as-a-service-raas-une-activite-illicite-qui-a-desormais-pignon-sur-rue

https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

https://www.lemondeinformatique.fr/actualites/lire-4-groupes-de-ransomwares-emergents-dangereux-a-surveiller-83944.html

https://www.darktrace.com/fr/blog/les-9-stades-des-ransomwares-comment-l-ia-repond-a-chaque-etape/

LA SCELTA EUROPEA
DELLA SICUREZZA INFORMATICA

WWW.STORMSHIELD.COM

Qualsiasi diffusione, riproduzione o rappresentazione, anche parziale, del presente white paper per scopi diversi dall'uso privato su qualsiasi supporto è vietata e può comportare la responsabilità civile e penale per chiunque non si attenga a tale divieto.

Copyright © 2022 Stormshield

STORMSHIELD